



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,213	02/05/2002	Siani Lynne Pearson	B-4488PCT 619500-7	8050
22879	7590	04/26/2006	EXAMINER	
HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400				AVERY, JEREMIAH L
ART UNIT		PAPER NUMBER		
		2131		

DATE MAILED: 04/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/049,213	PEARSON ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Jeremiah Avery	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 09 February 2006.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-44 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-44 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 05 February 2006 is/are: a) accepted or b) objected to by the Examiner.
 

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date: _____
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>03/17/06</u>	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

### **DETAILED ACTION**

1. Claims 1-44 have been examined.
2. Responses to Applicant's remarks have been given.

#### ***Drawings***

1. The drawings were received on 02/05/02. These drawings are unacceptable. While the applicant asserts that replacement drawings were supplied with the preliminary amendment filed on 02/05/02, the examiner will note that the said replacement drawings were not present with the corrected labels. In addition to Replacement Sheets containing the corrected drawing figure(s), applicant is required to submit a marked-up copy of each Replacement Sheet including annotations indicating the changes made to the previous version. The marked-up copy must be clearly labeled as "Annotated Sheets" and must be presented in the amendment or remarks section that explains the change(s) to the drawings. See 37 CFR 1.121(d)(1). Failure to timely submit the proposed drawing and marked-up copy will result in the abandonment of the application.
2. In order to avoid abandonment, the drawing informalities noted in the paper mailed on 10/06/05, must now be corrected. Correction can only be effected in the manner set forth in the above noted paper.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-15, 18-22, 24, 26-44 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,943,423 to Muftic, hereinafter Muftic.

3. (Original) Regarding claims 1, 18 and 27, Muftic discloses a computer system adapted to restrict operations on data, comprising:

a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data (column 3, lines 46-67, column 4, lines 1-10 and column 5, lines 23-54);

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49);

[Performing “cryptographic functions and transformations” assists in protecting the contents found in the trusted module (“smart token”).]

an access profile specifying license permissions of users with respect to the data (column 5, lines 48-54);

wherein the secure operator is adapted to check the access profile to determine whether a requested operation is licensed for the user identity contained in the portable trusted module and prevent the requested operation if a license is required and not present (column 5, lines 55-67 and column 6, lines 1-4, 19-31).

4. (Original) Regarding claims 2 and 28, Mufic discloses wherein the computer platform further comprises a platform trusted module and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication (Figure 1, column 3, lines 46-61, column 5, lines 30-47, column 7, lines 61-67 and column 8, lines 1-23).

5. (Original) Regarding claims 3, 29 and 42, Mufic discloses wherein some or all of the functionality of the secure operator is within the platform trusted module (column 3, lines 46-67 and column 4, lines 1-5).

6. (Original) Regarding claims 4 and 30, Mufic discloses wherein the access profile is within the computer platform (column 5, lines 30-47).

7. (Original) Regarding claims 5 and 31, Mufic discloses wherein some or all of the data is within the computer platform and the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data (column 3, lines 58-67, column 4, lines 1-5 and column 6, lines 31-31).

Art Unit: 2131

8. (Original) Regarding claim 6, Muftic discloses wherein some or all of the data is within the portable trusted module or in a device containing the portable trusted module and the portable trusted module or the device containing the portable trusted module further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data (column 6, lines 32-42, 47-49).

9. (Original) Regarding claims 7, 32 and 43, Muftic discloses wherein the data protector is within the relevant trusted module (column 3, lines 46-67, column 4, lines 1-5 and column 6, lines 31-31).

10. (Original) Regarding claims 8, 33 and 44, Muftic discloses wherein the data protector is adapted to check installation of data and to load a digest of protected data and/or any associated access profile into the relevant trusted component (column 8, lines 61-67, column 9, lines 1-17, 40-57).

11. (Original) Regarding claims 9 and 34, Muftic discloses wherein the trusted platform is adapted at boot to check the integrity of operation protection code comprising the secure operator and, if present, the data protector (column 5, lines 55-67, column 6, lines 1-4 and column 9, lines 7-13).

12. (Original) Regarding claim 10, Muftic discloses wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication and wherein the computer platform is adapted to perform the integrity check by reading and hashing the operation protection code to produce a first hash, reading and decrypting a stored signed version of a secure operation protection code hash using a public key certificate

Art Unit: 2131

of a third party stored in the platform trusted module to produce a second hash, and comparing the first has and the second hash (Figure 1, column 3, lines 46-61, column 5, lines 30-67, column 6, lines 1-4, column 7, lines 61-67, column 8, lines 1-23, column 15, lines 66 and 67 and column 16, lines 1-15 and 35-46).

13. (Original) Regarding claim 11, Muftic discloses wherein the portable trusted module contains a user access license specifying access rights to the data associated with the removable trusted module, whereby unless prevented by the access profile, the secure operator is adapted to check the user access license to determine whether a requested operation is licensed for the user identity contained in the portable trusted module (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10, column 5, lines 48-67 and column 6, lines 1-4, 19-49).

14. (Original) Regarding claims 12 and 35, Muftic discloses wherein the computer platform comprises a secure communication path between the platform trusted module and the operating system of the computer platform (column 5, lines 30-47 and column 8, lines 12-22).

15. (Currently Amended) Regarding claims 13 and 36, Muftic discloses wherein the computer platform is adapted such that:

the operating system requests a policy check from the secure operator before acting upon the data, by sending the name of the target data plus the intended operation (column 9, lines 47-57 and column 10, lines 38-41);

the secure operator checks the restrictions associated with the target data in the access profile, to determine whether the data may be operated upon (column 5, lines 55-67 and column 6, lines 1-4, 19-31);

the secure operator checks the proposed usage with the restrictions, and replies to the operating system (column 5, lines 48-54).

16. (Currently Amended) Regarding claims 14 and 37, Muftic discloses wherein the computer platform further comprises a platform trusted module, wherein the platform trusted module and the portable trusted module are adapted for mutual authentication and wherein some or all of the functionality of the secure operator is within the platform trusted module (Figure 1, column 3, lines 46-67, column 4, lines 1-5, column 5, lines 30-47, column 7, lines 61-67 and column 8, lines 1-23);

wherein on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure operator whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested (column 5, lines 48-67, column 6, lines 1-4, 21-31 and column 10, lines 5-20).

Art Unit: 2131

17. (Original) Regarding claim 15, Muftic discloses wherein the computer platform further comprises a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, and wherein the computer system further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data (Figure 1, column 3, lines 46-67, column 4, lines 1-5 column 5, lines 30-47, column 6, lines 31-31, column 7, lines 61-67 and column 8, lines 1-23);

wherein the relevant trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result (Figure 22, column 5, lines 55-67, column 6, lines 1-4, 21-31 and column 16, lines 35-46).

18. (Original) Regarding claim 19, Muftic discloses wherein the operating system of the computer platform is adapted to request a policy check from the access controller before carrying out certain operations on the data, whereupon the access controller checks restrictions applying to the data to determine whether the data may be operated on, and replies to the operating system accordingly (column 5, lines 30-67 and column 6, lines 1-4 ad 21-31).

19. (Currently Amended) Regarding claim 20, Muftic teaches a method of restricting operations on data in a system comprising:

a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data (column 3, lines 46-67, column 4, lines 1-10 and column 5, lines 23-54);

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49);

an access profile specifying license permissions of users with respect to the data (column 5, lines 48-54);

the method comprising a request for a policy check by the operating system of the computer platform to the secure operator before acting upon the data, by sending to the secure operator the name of the target data plus the intended operation (column 9, lines 47-57 and column 10, lines 38-41);

the secure operator checking the restrictions associated with the target data in the access profile to determine whether the data may be operated upon (column 5, lines 55-67 and column 6, lines 1-4, 19-31);

the secure operator checking the proposed usage with the restrictions, and replying to the operating system (column 5, lines 48-54).

20. (Original) Regarding claim 21, Muftic teaches wherein the computer platform further comprises a platform trusted module, and wherein some or all of the functionality of the secure operator is within the platform trusted module, and whereby on request by the operating system for permission to operate on the data, the secure operator sends a message to the access profile signed with a private key of the platform trusted module, wherein the access profile has access to the public key of the platform trusted module and can verify and authenticate the signed message with said public key, whereby if satisfied the access profile sends access profile data to the secure operator, whereupon the secure operator tests the access profile data and if appropriate requests the operating system to carry out the operation requested (column 3, lines 46-67, column 4, lines 1-5, column 5, lines 48-67, column 6, lines 1-4, 21-31 and column 10, lines 5-20).

21. (Original) Regarding claim 22, Muftic teaches wherein the computer platform further comprises a data protector for checking data integrity before a processor of the computer platform carries out operations on the data, and wherein the platform trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result (Figure 22, column 3, lines 58-67, column 4, lines 1-5, column 5, lines 55-67, column 6, lines 1-4, 31-31 and column 16, lines 35-46).

22. (Original) Regarding claim 24, Muftic teaches wherein the computer platform comprises a secure communication path between the platform trusted component and the operating system, and whereby the request from the secure operator to the

operating system to use the data is provided on the secure communication path (column 5, lines 30-47 and column 8, lines 12-22, 32-34).

23. (Original) Regarding claim 26, Muftic teaches a method of installing data on to a computer platform for restricted use thereon, the computer platform comprising:

a computer platform having a secure operator for checking whether a user of the platform is licensed to perform a requested operation on the data and for enabling use of the data, a platform trusted module wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification, and a data protector for checking data integrity before a processor of the computer platform carries out operations on the data (column 3, lines 38-67, column 4, lines 1-10, column 5, lines 23-54 and column 6, lines 32-49);  
the method comprising verification of the reliability of the data before installation of the data and an associated access profile, and loading of a digest of protected data and an associated access profile into the platform trusted module, whereby the digest is used by the data protector and/or secure operator before execution of the data (column 8, lines 61-67, column 9, lines 1-17, 40-57).

24. (Original) Regarding claim 38, Muftic discloses a platform trusted module, and wherein the platform trusted module and the portable trusted module are adapted for mutual authentication, wherein the platform trusted component contains a secure result of a one-way function on the data and associated access profile, and the data protector

Art Unit: 2131

prevents the operation from being carried out if calculation of the one-way function provides a result different from the secure result (Figure 1, column 3, lines 46-61, column 5, lines 30-47, 55-67, column 6, lines 1-4, 31-31, column 7, lines 61-67, column 8, lines 1-23 and column 16, lines 35-46).

25. (Currently Amended) Regarding claim 39, Muftic discloses a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49);

the portable trusted module containing a user access license specifying access rights to data associated with the portable trusted module (column 5, lines 48-54).

26. (Original) Regarding claim 40, Muftic discloses a portable trusted module located within a smart card (column 2, lines 28-30, column 3, lines 26-28, 38-45 and column 4, lines 6-10).

27. (Original) Regarding claim 41, Muftic teaches a method of restricting operations on data in a system comprising:

a computer platform having an access controller specifying license permissions of users with respect to the data (column 3, lines 46-67, column 4, lines 1-10 and column 5, lines 23-54);  
enabling use of the data (column 5, lines 48-54, "authorizing the activity");

a portable trusted module containing a user identity, wherein a trusted module is a component adapted to behave in an expected manner and resistant to unauthorized external modification (column 2, lines 28-30, column 3, lines 26-28, 38-42, column 4, lines 6-10 and column 6, lines 32-49);  
the method comprising a request for a policy check by the operating system of the computer platform to the access controller before acting upon the data, by sending to the access controller the name of the target data plus the intended operation (column 9, lines 47-57 and column 10, lines 38-41);  
the access controller checking the restrictions associated with the target data to determine whether the data may be operated upon (column 5, lines 55-67 and column 6, lines 1-4, 19-31);  
replying to the operating system (column 5, lines 48-54, column 6, lines 25-31). [A response is given in the form of "authorizing" or denying access to the data.]

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Art Unit: 2131

28. (Original) Claims 16 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic as applied to claims 2 and 21 above (respectively), and further in view of U.S. Patent No. 6,091,835 to Smithies et al., hereinafter Smithies.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

29. As per claims 16 and 25, Muftic discloses the invention substantially as claimed in claims 2 and 21, respectively, but fails to disclose wherein the platform trusted component is adapted to log requests to the operating system to perform particular operations on the data.

30. However, Smithies discloses wherein the platform trusted component is adapted to log requests to the operating system to perform particular operations on the data (column 11, lines 51-67, column 16, lines 39-60, column 19, lines 16-24, column 26, lines 37-42, column 27, 49-60, column 42, lines 53-67 and column 43, lines 1-11).

31. The motivation to do so would be to "confirm specifics such as that the affirming party is in fact the identified party" (Smithies - column 7, lines 23-25, column 8, lines 15-43, column 9, lines 64-67 and column 10, lines 1-13).

32. Therefore, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to employ the teachings of Smithies within the system of

Muftic to obtain the claimed invention because it would restrict access to the desired data, document, etc. to only those possessing authorized access credentials.

33. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic as applied to claim 6 above, and further in view of U.S. Patent No. 6,091,835 to Smithies et al., hereinafter Smithies.

34. As per claim 17, Muftic discloses the invention substantially as claimed in claim 6, but fails to disclose wherein the portable trusted component is adapted to log requests to the operating system to perform particular operations on the data.

35. However, Smithies discloses wherein the portable trusted component is adapted to log requests to the operating system to perform particular operations on the data (column 11, lines 51-67, column 16, lines 39-60, column 19, lines 16-24, column 26, lines 37-42, column 27, 49-60, column 42, lines 53-67 and column 43, lines 1-11).

36. The motivation to do so would be to "confirm specifics such as that the affirming party is in fact the identified party" (Smithies - column 7, lines 23-25, column 8, lines 15-43, column 9, lines 64-67 and column 10, lines 1-13).

37. Therefore, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to employ the teachings of Smithies within the system of Muftic to obtain the claimed invention because it would restrict access to the desired data, document, etc. to only those possessing authorized access credentials.

38. (Original) Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic as applied to claim 21 above, and further in view of U.S. Patent No. 5,870,723 to Pare et al., hereinafter Pare.

Art Unit: 2131

39. As per claim 23, Muftic discloses the invention substantially as claimed in claim 21, but fails to teach wherein before execution of the data, the data protector checks that there are not multiple copies of the data stored within the computer platform and prevents data execution if there are multiple copies.

40. However, Pare teaches wherein before execution of the data, the data protector checks that there are not multiple copies of the data stored within the computer platform and prevents data execution if there are multiple copies (column 13, lines 12-19, 26-49). Pare only allows one copy of data and other software to be stored, thus preventing multiple copies from existing.

41. The motivation to do so would be "that even successful capture and dissection of a given future key table does not reveal messages that were previously sent" (column 19, lines 43-57).

42. Therefore, it would have been obvious to one ordinarily skilled in the art at the time the invention was made to employ the teachings of Pare within the system of Muftic to obtain the claimed invention because it would better resist attempts to obtain access to protected via a stolen access code, identifier, credential, etc.

***Double Patenting***

A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

43. Claim 27 is provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claim 27 of copending Application No. 10/049211. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

44. The referenced application (10/049211, hereinafter "211") anticipates the invention disclosed in this application, hereinafter "213" as follows:

45. Both "211" and "213" disclose a trusted module found within the platform.

46. The "removable, trusted module" of "211" is the same as the "portable trusted module" found in "213" for the portability of the module in "213" indicates that it can, in fact, be removed as found in "211". These are synonymous terms.

47. Within "211", it is inherent that a form of "access profile" as mentioned in "213" is required when performing "the license-check with reference to the user identity" of "211". A check occurs by conducting a comparison of the given credentials with those within a profile containing a list, table, etc. of users that are licensed to use the particular

data. Hence, an “access profile” of some sort would exist within the invention found in “211”.

48. The “secure operator” of “213” is a generic form of the “secure executor” of “211”, thus a genus-species relationship is established between the two applications.

49. There is an explicit and implicit relationship between these two applications regarding the success and prevention of access to the requested operation/data. Within “213” there is an explicit recitation relating to the lack of success of the licensing of a user ID regarding the requested operation, in the form of the trusted module being able to “prevent the requested operation if a license is required and not present.” It would be inherently understood that while prevention will occur; successful access to the requested operation would occur, pending a successful license-check. In “211”, the success of obtaining access is explicitly stated with respect to the license check of the user identity. It would be inherent that should there be a failure in licensing the requested operation for the user identity given, that the trusted module would perform a function/operation that would prevent said user from obtaining unlicensed access to any operation and/or data found within the platform.

50. Similar anticipatory arguments between “211” and “213” can be made regarding claims 1, 2 and 4 of “213”.

#### ***Response to Arguments***

51. Applicant’s arguments, see page 15, filed 02/09/06, with respect to the objections to the specification have been fully considered and are persuasive. The objections of the specification have been withdrawn.

52. Applicant's arguments, see page 15, filed 02/09/06, with respect to objections to claims 13, 14, 20, 22, 36 and 41 have been fully considered and are persuasive. The objections of claims 13, 14, 20, 22, 36 and 41 have been withdrawn.

53. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. With regards to the arguments pertaining to the drawings, the examiner maintains the objection to the drawings based upon the above-cited grounds.

54. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. With regards to the "portable trusted module" as claimed by the applicant in claims 1, 18, 27 and 39, the disclosure of smart cards and PCMCIA cards, as broadly interpreted by the examiner, by Muftic discloses said "portable trusted module". Also the "cryptographic functions" as disclosed by Muftic could be utilized in the prevention of "unauthorized external modification".

55. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. With regards to the "access profile specifying license permissions" as claimed by the applicant, a license can be a certification of authority which would allow a specific user(s) to be able to engage in designated activities, as granted by said authority. Thus, the "authorization credentials" as disclosed by Muftic are broadly interpreted by the examiner as pertaining to, inter alia, "license permissions".

Furthermore, an "access profile" exists within the teachings of Muftic for in order to determine whether or not a user can obtain access, a set of credentials and identification means are stored and associated with each user, thus providing the

creation of a form of an "access profile" which will either allow or restrict access, dependent upon, inter alia, said credentials.

56. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. With regards to the "platform trusted module" of claims 2 and 28, Muftic discloses using a "computer or network resource" as well as a "computer equipped device". These, among other devices disclosed by Muftic, provide an environment for which authorization attempts, public/private key cryptography, generating digital signature keys and other such security aspects to be implemented.

57. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. With regards to "wherein some or all of the functionality of the secure operator is within the platform trusted module" as found in claims 3, 29 and 42, the examiner maintains that the "computer" as disclosed my Muftic contains functionality that allows "access to a set of secure transaction services, including secret key and/or public key cryptographic services" (column 3, lines 56-58).

58. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. With regards to claims 20 and 41, the examiner maintains that Muftic discloses the claimed invention. The "user identity" is disclosed by Muftic in the form of "user identification and a user random number" as cited in column 5, line 36. Also, the "activation and access test" as disclosed by Muftic can be utilized for "access control purposes" which pertains to the embodiment as claimed in the present invention, "the secure operator checking the restrictions associated with the target data in the access

profile to determine whether the data may be operated upon". Furthermore, the "interrogation/response mode" can be used for, inter alia, policy checking.

Additionally, pertaining to claim 41, regarding "replying to the operating system", a response is given in the form of "authorizing" or denying access to the data. Also, Muftic discloses interacting with a system running MS Windows, a known operating system (column 8, lines 35-48).

59. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. As per the limitation, "verification of the reliability of the data before installation of the data and an associated access profile" found in claim 26, the examiner maintains that the "interrogation/response mode" as disclosed by Muftic acts as a form of verification for the particular configuration file. Also, with the "user's certificate(s) (certification authority)" as cited in column 10, lines 30-41, "a digest of protected data and an associated access profile" are hereby disclosed by Muftic.

60. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. Pertaining to the 35 USC 103 rejection of claims 16, 17, 23 and 25, the examiner maintains that Muftic, as broadly interpreted by the examiner, anticipates the claims upon which claims 16, 17, 23 and 25 draw dependency from. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art.

See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the references utilized for the above cited grounds of rejection provide proper motivation for combining said references.

61. Applicant's arguments filed 02/09/06 have been fully considered but they are not persuasive. With regards to the Double Patenting rejection of claim 27, the examiner respectfully maintains the rejection. First, the applicant asserts the dependency of claim 27 to claim 20, of which this is erroneous for claim 27 claims dependency to claim 21. Further, the table below will further illustrate the similarities between claim 27 of application "213" and that of claim 27 for application "211".

<u>Claim 27 for Application "213"</u>	<u>Claim 27 for Application "211"</u>
Portable trusted module	Removable, trusted module
Secure operator	Secure executor

Usage of synonymous terms does not differentiate each application for patentability.

The examiner upholds the previously stated additional reasoning for making the Double Patenting rejection.

### ***Conclusion***

62. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

63. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

64. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeremiah Avery whose telephone number is (571) 272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

65. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

66. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JLA

CHRISTOPHER REVAK  
PRIMARY EXAMINER

*ClL 4/24/06*

Application/Control Number: 10/049,213

Art Unit: 2131

Page 24